Preventing a cyber zombie apocalypse

April 8, 2018

Preventing a cyber zombie apocalypse

by Neale Pickett

Cybercrime rates are on the rise, but what exactly does that mean? Cybercrime is any sort of crime using a computer—simple enough. And now that most people in the United States have a computer or access to one, cybercrime is more common than ever.

Say, for instance, someone wanted to take down a popular website through what's called a distributed denial-of-service, or DDoS, attack. An example of this is the 2016 DDoS attack on the internet performance management company DYN that temporarily took down more than 75 major websites.

A single computer could not possibly do something like the DYN attack on its own, but cybercriminals aren't using just one. They infect thousands of computers with malware to create a network of computers called a botnet. This botnet is a sort of zombie army that stands by waiting for commands and can be sold to bidders to do whatever a bad actor wants.

This person could recruit the zombie army, which would then do whatever they're told, rather than what each one of their users thinks they should be doing. The bad guys could direct all 50,000 computers to go to the site at once — that denial-of-service attack would crash the site, taking it off the internet.

Attacks like these are the reason Los Alamos National Laboratory has been working on cybersecurity techniques, processes and tools to prevent and detect cyberattacks.

This story first appeared in Santa Fe New Mexican.